

# Socket

Care must be exercised when a process with elevated permissions grants or allows children processes to inherit its rights.

Sean Barnum, Cigital, Inc. [vita<sup>1</sup>]

Copyright © 2007 Cigital, Inc.

2007-04-17

## Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 2575 bytes

Attack Category	<ul style="list-style-type: none"><li>Denial of Service</li></ul>		
Vulnerability Category	<ul style="list-style-type: none"><li>Privilege escalation problem</li></ul>		
Software Context	<ul style="list-style-type: none"><li>Inheritance</li><li>Networking</li></ul>		
Location	<ul style="list-style-type: none"><li>sys/socket.h</li></ul>		
Description	<p>Care must be exercised when a process with elevated permissions grants or allows children processes to inherit its rights.</p> <p>The socket function creates an endpoint for communication and returns a descriptor to the calling process.</p> <p>An inherited socket with broad permissions (e.g., root) could enable the establishment of a privileged connection to another machine making it vulnerable to further attack.</p>		
APIs	Function Name	Comments	
	socket()		
Method of Attack	An attacker can cause a denial-of-service using ioctl functions with the children of a process that have inherited a socket from a root process.		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
	Always	Avoid giving un-trusted child processes sockets with root privileges.	Effective if malicious child processes are not given sockets with root access.
Signature Details			
Examples of Incorrect Code			

1. <http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html> (Barnum, Sean)

<b>Examples of Corrected Code</b>	
<b>Source References</b>	<ul style="list-style-type: none"> <li>• <a href="http://unixhelp.ed.ac.uk/CGI/man-cgi?socket+2">http://unixhelp.ed.ac.uk/CGI/man-cgi?socket+2</a></li> <li>• <a href="#">ITS4 Source Code Vulnerability Scanning Tool</a></li> </ul>
<b>Recommended Resource</b>	
<b>Discriminant Set</b>	<b>Operating System</b>
	<b>Language</b>

## Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at [copyright@cigital.com](mailto:copyright@cigital.com)<sup>1</sup>.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

---

1. <mailto:copyright@cigital.com>